COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

ANNUAL REPORT

2012-2013

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1984, Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: 613-992-3044
Fax: 613-992-4096
Website: www.ocsec-bccst.gc.ca

© Minister of Public Works and
Government Services 2013
Cat. No. D95-2013
ISSN 1206-7490

Cover design: Cameron Fraser

Communications Security
Establishment Commissioner

The Honourable Robert Décary, Q.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

June 2013

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Minister:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you my annual report on my activities and findings for the period of April 1, 2012, to March 31, 2013, for your submission to Parliament.

Yours sincerely,

Robert Décary

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE OF CONTENTS

BIOGRAPHY OF THE HONOURABLE ROBERT DÉCARY, Q.C.

The Honourable Robert Décary, Q.C., was appointed Commissioner of the Communications Security Establishment on June 18, 2010, for a three-year term.

Commissioner Décary was born in Montréal in 1944. He received his education at Collège Jean-de-Brébeuf (BA), at Université de Montréal (LL.L.) and the University of London (LL.M.). He was called to the Barreau du Québec in 1967 and named Queen's Counsel in 1986.

In the course of a career dedicated to public office, the law and journalism, he was Special Assistant to the Honourable Mitchell Sharp (then Canada's Secretary of State for External Affairs) (1970–1973), Co-Director for Research on the Task Force on Canadian Unity, the Pepin-Robarts Commission (1978–1979) and member of the French Constitutional Drafting Committee of the federal Department of Justice (1985–1990).

He practised law in Montréal, then in Gatineau, where, in the firm Noël, Décary, he specialized in representing many law offices and the Attorney General of Québec before the Supreme Court of Canada.

He has written a number of feature articles for *Le Devoir* and *La Presse*, and has contributed to many legal journals and textbooks. He is the author of *Aide-mémoire sur la Cour suprême du Canada* (1988) and of *Chère Élize* (or *The Long and the Short History of the Repatriation*) (1983).

He was a member of the Federal Court of Appeal from 1990 to 2009. In 2009, he was appointed arbitrator of the Court of Arbitration for Sport in Lausanne, Switzerland, and in 2010 he became a member of the Sport Dispute Resolution Centre of Canada.

COMMISSIONER'S MESSAGE: A SUMMARY AT THE END OF MY TERM

When the Minister of National Defence tables this annual report before Parliament, I will have completed my three-year term as Communications Security Establishment (CSE) Commissioner. For personal reasons I declined an offer to renew my mandate. This message affords me an opportunity to reflect on my time as the head of the Office of the CSE Commissioner.

Reports and recommendations

During my tenure as Commissioner I submitted to the Minister of National Defence 19 review reports, covering almost every aspect of the activities of Communications Security Establishment Canada (CSEC), including those carried out under ministerial authorizations or at the request of law enforcement and security agencies. Among the activities reviewed were those relating to the collection of foreign signals intelligence, the protection of electronic information and information infrastructures considered important by the Government of Canada, and technical and operational assistance provided by CSEC, notably to the Canadian Security Intelligence Service (CSIS). My reports contained 12 recommendations.

The integrity of the review process and the credibility of the Commissioner's office depend in large part on the follow-up by the office of CSEC's implementation of Commissioners' recommendations. I am pleased to note that since 1997, fully 92 percent (127 of 138) of Commissioners' recommendations in 74 classified reports submitted to the Minister have been accepted and implemented, or are being addressed. This means, *inter alia* that measures to protect the privacy of Canadians are continually being adapted and refined to reflect the ever-changing technological and operational environment in which CSEC must work. Indeed, some Commissioners' recommendations have resulted in CSEC suspending certain activities to re-examine how the activities are conducted and, in other instances, have led to important improvements to CSEC policies and practices.

Maintaining healthy relations with CSEC

It strikes me as vital that an organization under independent review and the review body itself cultivate a relationship built on respect and good faith. By law, CSEC must take measures to protect the privacy of persons in Canada and Canadians, wherever in the world they may be. By law, the Commissioner must ensure that CSEC meets this obligation. The protection of privacy is therefore a shared objective of our two organizations. I also consider it essential that our relationship be one of complementarity rather than superiority. With my years of experience, I see the office more as CSEC's conscience than as a sword of Damocles, and I believe that CSEC increasingly sees it this way as well.

I can say with confidence that CSEC's Chiefs during my time as Commissioner, John Adams initially and then John Forster, have spared no effort to instill within CSEC a culture of respect for the law and for the privacy of Canadians. Both men have been honest in their dealings with me, sometimes tough, but always acting in good faith.

Transparency

From the start of my time as Commissioner, I have sought to demystify, within the unavoidable constraints of national security and public safety, the culture of secrecy pervading the activities of security and intelligence agencies. I believe I have succeeded to some degree, based on the feedback that my annual reports have been more informative, more understandable, and have brought clarity to many of the activities of my office and of CSEC. Much remains to be done, but I believe that the ice has been broken and that the security and intelligence agencies understand they can speak more openly about their work without betraying state secrets or compromising national security. The greater the transparency, the less sceptical and cynical the public will be.

It is in this context of transparency that the Commissioner's office organizes periodic luncheon meetings with outside experts in the fields of national security and privacy. This facilitates greater understanding on their part of how we go about our work, and we in turn learn about their perspectives and interests.

Review bodies working cooperatively

My office and the Security Intelligence Review Committee (SIRC) have similar functions but are subject to different legislation. CSEC and CSIS also have different legislation but their respective laws authorize cooperation between them, whereas the legislation governing my office and SIRC does not contain similar provisions. This means that where CSEC and CSIS cooperate and conduct joint activities, my office and SIRC do not have an equivalent authority to conduct joint reviews. Nonetheless, I believe a certain amount of collaboration among review bodies is possible under existing legislation. For example, where I have no mandate to follow-up, I may refer questions to SIRC that concern CSIS. Activities beyond this, such as the sharing of special operational information of the agencies, may require the intervention and approval of Cabinet, and possibly also legislative change. Ideally, the law should authorize, even encourage, such cooperation.

The creation of an over-arching structure that would group existing review bodies under a single umbrella, proposed in a past commission of inquiry report, does not strike me as a sensible solution at this point. Before we create an additional super-bureaucracy, with the associated burden and costs, we may be better advised to optimize existing review bodies and facilitate their collaboration.

Another form of cooperation among security and intelligence review bodies has occurred over the past few years. My office has provided an introductory training course for new employees of security and intelligence review bodies, to explain various review methods and to contribute to the development of more rigorous review practices.

Information sharing with international partners

The growth of international cooperation in the intelligence field has important implications for privacy. We want to ensure that the foreign countries and organizations with which Canada exchanges information protect privacy with as much rigour as Canada exercises. This is not an easy task. On the one hand, nations are sovereign and do not appreciate interference in their internal affairs, particularly not in the area of security. On the other hand, review bodies and mechanisms vary from country to country. In the absence of international intelligence review standards, I believe the best guarantee of the protection of the privacy of Canadians in information exchanged with international partners lies in promoting and ensuring strong and independent review bodies in those countries. We are, in fact, already doing this to some extent.

For the past 15 years, the review bodies of a dozen countries, including members of the "Five-Eyes" countries (Canada, the United States, the United Kingdom, Australia and New Zealand), have attended a biennial conference. These meetings have been a source of rewarding exchanges and new inspiration. The sharing of perspectives and best practices is a stimulating and enriching experience. As well, countries for which independent intelligence review is in its early stages may be invited to attend the conferences as observers and gain knowledge about what is happening elsewhere. Canada hosted this conference in May 2012.

On the bilateral level, my office meets with representatives of foreign review bodies and oversight committees. This past year, for example, I met with members of a delegation of French parliamentarians seeking information on the nature and methodology of Canadian review bodies. I have also met with members of the Belgian Standing Intelligence Agencies Review Committee and the British Intelligence and Security Committee. It is my wish that these kinds of beneficial meetings occur more frequently.

Cyber security and cyber attacks

One can no longer talk about security without mentioning cyber threats. Barely a week goes by without headlines dealing with the risk of breaches of public and private computer systems. CSEC, by its very mandate, is called on to play a leadership role in protecting electronic information and information infrastructures of importance to the Government of Canada. CSEC may also lend its experience to assist Public Safety Canada in its role of helping to protect critical infrastructure that may involve the private sector.

It is unavoidable that CSEC may unintentionally intercept the private communications of Canadians while conducting certain information technology (IT) security activities. For this reason, in recent years, the Commissioner's office has increased its vigilance in this area, completing a number of reviews, while others have been initiated; I have no doubt that my successor will continue this work.

Proposals for legislative changes to the *National Defence Act*

I started my mandate with the expectation that the legislative amendments to the *National Defence Act* proposed by my predecessors would soon be introduced in Parliament, but this has yet to happen. I am deeply disappointed at the lack of action by the government, which is no longer in a minority situation, to address the ambiguities identified by my predecessors and myself. These amendments — as I have said many times before — would improve the provisions that were hastily

enacted in the aftermath of September 11, 2001. The proposals to address the issues raised by Commissioners should not, in my opinion, be controversial.

The independence of the Office of the CSE Commissioner

The office attained its institutional and financial independence just over five years ago when it received its own funding approved by Parliament, and was no longer part of the budget of the Department of National Defence. To emphasize this independence, 2011 marked the first time the Commissioner issued his own news release to highlight the tabling in Parliament of his annual report by the Minister of National Defence. Financial independence, however, does have its drawbacks. As a result of having its own appropriation, the Commissioner's office, a micro-agency with a budget of roughly two million dollars, is subject to the same accounting and reporting requirements as all departments, each with their individual budgets, some into the billions. To my mind, this is an example of excessive bureaucracy that has resulted in a significant level of reporting that is of limited value to both the office and its stakeholders.

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

My mandate under the *National Defence Act* consists of three key functions:

1. **reviewing CSEC activities** to determine whether they comply with the law;

2. **conducting investigations** I deem necessary in response to complaints about CSEC; and

3. **informing the Minister** of National Defence (who is accountable to Parliament for CSEC) and the Attorney General of Canada of any CSEC activities that I believe may not be in compliance with the law.

Under the *Security of Information Act*, I also have a mandate to receive information from persons who are permanently bound to secrecy if they believe it is in the public interest to release special operational information of CSEC. (More information on the Commissioner's responsibilities for public interest defence is available on the office's website.)

CSEC's mandate

When the *Anti-terrorism Act* came into effect on December 24, 2001, it added Part V.1 to the *National Defence Act*, and set out CSEC's three-part mandate:

- part (a) authorizes CSEC to acquire and use foreign signals intelligence in accordance with the Government of Canada's intelligence priorities;
- part (b) authorizes CSEC to help protect electronic information and information infrastructures of importance to the Government of Canada; and
- part (c) authorizes CSEC to provide technical and operational assistance to federal law enforcement and security agencies, including helping them obtain and understand communications collected under those agencies' own lawful authorities.

Reviewing CSEC activities

My mandate to review CSEC activities relates to CSEC collecting foreign signals intelligence, protecting electronic information and information infrastructures of importance to the Government of Canada, and assisting federal law enforcement and security agencies.

The purpose of my review mandate is:

- to determine whether the activities conducted by CSEC under ministerial authorization are, in fact, those authorized by the Minister of National Defence, and to verify that the conditions for authorization required by the *National Defence Act* are met;
- to determine whether CSEC complies with the law and, if I believe that it may not be complying, to report this to the Minister of National Defence and to the Attorney General of Canada;
- to verify that CSEC does not direct its foreign signals intelligence and IT security activities at Canadians; and
- to promote the development and effective application of satisfactory measures to protect the privacy of Canadians in all the activities CSEC undertakes.

Protection of Canadians

CSEC is prohibited by law from directing its foreign signals intelligence collection and IT security activities at Canadians — wherever they might be in the world — or at any person in Canada.

Ministerial authorizations

The *National Defence Act* allows the Minister of National Defence to give CSEC written ministerial authorization to unintentionally intercept private communications while collecting foreign signals intelligence or

while protecting computer systems of the Government of Canada from mischief, unauthorized use or interference. In each case, the law specifies the conditions under which a ministerial authorization can be issued. Ministerial authorizations relate to an activity or class of activities specified in the authorizations — that is, to a specific method of acquiring foreign signals intelligence or of protecting computer systems (the how); however the authorizations do not relate to a specific individual or subject (the whom or the what). The law also directs the CSE Commissioner to review activities carried out under a ministerial authorization and to report annually to the Minister on the review. (More information on ministerial authorizations as well as on the authorities for and limitations on CSEC activities are available on the office's website.)

Selection of activities for review

I use a risk-based and preventative approach to my reviews. I prioritize CSEC activities where risk is greatest for potential non-compliance with the law, including for risks to the privacy of Canadians, by considering, among other factors:

- the controls placed by CSEC on the activity to ensure compliance with legal, ministerial and policy requirements;
- whether the activity does, or has the potential to, involve private communications or information about Canadians;
- whether the activity is new, has changed significantly, or has had a lengthy period elapse since its last in-depth review;
- whether there have been significant changes to the authorities or technologies relating to the activity;
- whether Commissioners have made findings or recommendations relating to the activity that require follow-up; and
- issues arising in the public domain.

Information about Canadians: any personal information (as described in the *Privacy Act*) about a Canadian, or business information about a Canadian corporation.

Review methodology and criteria

My reviews of activities are *ex post*, that is, of activities that have occurred in the past. However, reviews always include an examination of CSEC's *ex ante* reasons for conducting the activities — to confirm that CSEC's justifications for the activities are lawful and within CSEC's mandate. In conducting a review, my office examines CSEC's hard-copy and electronic information and records, as well as CSEC's policies and procedures and legal advice received from Justice Canada. My employees request briefings and demonstrations of specific activities, interview CSEC managers and employees, and observe CSEC operators and analysts first hand to verify how they conduct their work. My employees test information obtained against the contents of CSEC's systems and databases.

Each review includes an assessment of CSEC activities against a standard set of criteria, described below, consisting of legal requirements, ministerial requirements, and policies and procedures. Each review may have additional criteria added, as appropriate.

Legal requirements: I expect CSEC to conduct its activities in accordance with the *National Defence Act*, the *Canadian Charter of Rights and Freedoms*, the *Privacy Act*, the *Criminal Code*, and any other relevant legislation, and in accordance with Justice Canada advice.

Ministerial requirements: I expect CSEC to conduct its activities in accordance with ministerial direction, following all requirements and limitations set out in a ministerial authorization or directive.

Policies and procedures: I expect CSEC to have appropriate policies and procedures in place to guide its activities and to provide sufficient direction on legal and ministerial requirements including the protection of the privacy of Canadians. I expect CSEC employees to be knowledgeable about and comply with policies and procedures. I also expect CSEC to have an effective compliance validation framework and activities to ensure the integrity of operational activities is maintained, including appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

My classified review reports document CSEC activities and practices and contain findings relating to the above-noted criteria. These reports may also disclose the nature and significance of deviations from the criteria. In some cases, I make recommendations to the Minister that are aimed at correcting discrepancies between CSEC activities and the expectations established by the review criteria.

The logic model in **Annex A** provides a flow chart of the review program (p. 41).

Horizontal reviews

Horizontal reviews examine processes common to all CSEC foreign signals intelligence collection methods or to IT security activities. For example, the processes by which CSEC:

- identifies, selects and directs its activities at foreign entities of intelligence interest located outside Canada or at threats to Government of Canada computer systems;
- uses, shares, reports, retains or disposes of intercepted information; or
- takes measures to protect private communications intercepted unintentionally and to protect information about Canadians.

Conducting investigations

My mandate includes undertaking any investigation I deem necessary in response to a written complaint — for example to determine whether CSEC has engaged, or is engaging, in unlawful activity or is not taking sufficient measures to protect the privacy of Canadians. (More information on the Commissioner's responsibilities for conducting investigations into complaints is available on the office's website.)

Informing the Minister

Under my mandate to keep the Minister of National Defence informed, I:

- forward the results of my reviews, in classified reports, to the Minister; and
- submit an unclassified report to the Minister on my activities each year, which the Minister must then table in Parliament. This is the 17th annual report.

While it is my primary duty to report any non-compliance by CSEC, a necessary element of my mandate also includes informing the Minister of any activities that I believe might present, or have the potential to present, a risk of non-compliance, such as an unlawful interception of a private communication or other invasion of the privacy of a Canadian. A number of my reports have included recommendations aimed at prevention. It is a goal of the Commissioner's office to strengthen CSEC practices that contribute to compliance and incorporate measures that protect the privacy of Canadians.

Independence

While I submit my reports to the Minister of National Defence, who is responsible for CSEC, my office is completely independent and receives its own funding from Parliament. My mandate is supported by the powers I have under the *Inquiries Act*, including the power of subpoena, to ensure access to all CSEC information and employees.

CSE Commissioner

The Commissioner is an independent statutory officer and is not subject to general direction from the Prime Minister, the Minister of National Defence or any other ministers on how to carry out his mandate. The Commissioner assists the Government of Canada in its control of CSEC by providing advice to the Minister to support the Minister's decision making and accountability for CSEC. The Commissioner's classified reports to the Minister and unclassified annual report, through the Minister to Parliament and the public, state whether CSEC has acted lawfully and the extent to which it protected the privacy of Canadians in the conduct of its activities.

Annex B contains the text of the relevant sections of the *National Defence Act* and the *Security of Information Act* relating to my role and mandate as CSE Commissioner (p. 43). (Information on the history of the Office of the CSE Commissioner is available on the office's website.)

COMMISSIONER'S OFFICE

Last year, work was completed on the expansion of the physical space of the office, to provide sufficient accommodation for existing functions, and for additional responsibilities resulting from the office receiving its own appropriation from Parliament. The expansion will allow me to hire two additional review officers to enable adequate review of CSEC, which has experienced significant growth. I have been supported in my work by a staff of eight, together with a number of subject-matter experts, as required. In 2012–2013, my office's expenditures were $2,285,718, which is within the overall funding approved by Parliament.

Annex C provides the 2012–2013 Statement of Expenditures for the Office of the CSE Commissioner (p. 47).

IMPACT OF COMMISSIONERS' RECOMMENDATIONS

Since 1997, my predecessors and I have submitted to the Minister of National Defence 74 classified review reports. In total, the reports contained 138 recommendations. CSEC has accepted and implemented or is working to address 92 percent (127 out of 138) of these recommendations.

Commissioners monitor how CSEC addresses recommendations and responds to negative findings as well as areas for follow-up identified in past reviews. This past year, CSEC advised my office that work had been completed in response to 14 past recommendations. Notably, CSEC implemented recommendations by:

- providing support to the Minister of National Defence to update certain ministerial directives;
- updating general memoranda of understanding for the exchange of information and operational cooperation with CSIS and Foreign Affairs and International Trade Canada;
- committing to report to the Minister of National Defence certain information (that cannot be publicly identified for security reasons), as a measure to protect the privacy of Canadians and to support the Minister in his accountability for CSEC;
- promulgating a revised policy for operational assistance to law enforcement and security agencies under part (c) of CSEC's mandate, including guidance on the retention and disposition of records relating to any assistance;
- promulgating a revised procedure that defines risk and risk mitigation for certain foreign signals intelligence collection activities as well as adopting a risk management framework for the planning and approval of these activities; and

- launching a new secure system with other government departments and agencies for handling and tracking requests for and disclosures of suppressed Canadian identity information.

These actions by CSEC demonstrate that review works. The Commissioner's office will examine the impact of these enhancements on compliance and privacy protection in future reviews. In addition, the Commissioner's office is monitoring six active recommendations that CSEC is working to address. The Minister's responses to two recommendations of this year were not received by the time this report was completed.

The office's website provides a complete list of the 74 classified review reports submitted to the Minister of National Defence.

OVERVIEW OF 2012–2013 FINDINGS AND RECOMMENDATIONS

During the 2012–2013 reporting year, I submitted six reports to the Minister of National Defence on my review of CSEC activities.

These reviews were conducted under two areas of my mandate:

- ensuring CSEC activities are in compliance with the law — as set out in paragraph 273.63(2)(*a*) of the *National Defence Act*; and
- ensuring CSEC activities under a ministerial authorization are authorized — as set out in subsection 273.65(8) of the *National Defence Act*.

The results

Each year, I provide an overall statement on my findings about the lawfulness of CSEC activities. With the exception of one review described below — in which I was unable to reach a definitive conclusion about compliance or non-compliance with the law for certain CSEC foreign signals intelligence activities — all of the activities of CSEC reviewed this past year complied with the law.

As well, this year, I made four recommendations to promote compliance with the law and to strengthen privacy protection. The recommendations, which are described in the following review summaries, relate to reinforcing policy guidance and expanding an existing practice on privacy protection to other circumstances, as well as providing the Federal Court of Canada with certain additional evidence about the nature and extent of the assistance CSEC may provide to CSIS.

Additionally, I forwarded to the Chair of SIRC, for information, certain general points relating to CSIS that arose out of the recommendations I made and that SIRC may wish to examine as it deems appropriate. This demonstrates how existing review bodies can, in the spirit of the recommendations of the commission of inquiry led by the Honourable Justice Dennis O'Connor, collaborate under existing legislation in the conduct of reviews of activities involving more than one security and intelligence agency.

Two reviews this year — the review of certain foreign signals intelligence activities and the review of CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the *Canadian Security Intelligence Service Act* (*CSIS Act*) — identified the absence of certain historical information in a CSEC system and database relating to foreign signals intelligence collection. This system and database support the process by which CSEC determines that entities of foreign intelligence interest are indeed foreign and located

outside of Canada, as required by the *National Defence Act*. The absence of the information limited my ability to assess the lawfulness of the CSEC activities in question, and could also affect review of other activities of CSEC. Due to the seriousness of this development, I directed my employees to conduct an in-depth examination of the issue to determine the implications and advise on a resolution. This issue added to the time required to complete these two reviews. It is encouraging that CSEC has already taken action and continues to do so to ensure the availability of information that is required for accountability and to demonstrate compliance with the law. The Commissioner's office will monitor developments.

In last year's annual report, I expressed frustration about a reduction in CSEC support to my office resulting in excessive delays in being able to proceed with some reviews. CSEC has taken steps to correct this situation and I am optimistic that these will result in a productive year ahead.

HIGHLIGHTS OF THE SIX REVIEWS SUBMITTED TO THE MINISTER IN 2012–2013

1. Review of certain foreign signals intelligence activities

Background

I examined CSEC's acquisition, use and exchange of information relating to certain foreign intelligence activities that occurred a number of years ago.

Findings and recommendations

I had no concern with respect to the majority of the CSEC activities reviewed. However, a small number of records suggested the possibility that some activities may have been directed at Canadians, contrary to law. A number of CSEC records relating to these activities were unclear or incomplete. After in-depth and lengthy review, I was unable to reach a definitive conclusion about compliance or non-compliance with the law.

In the process of review, I found that a number of CSEC records relating to exchanges of information with CSIS were sometimes unclear, which led me to recommend that CSEC promulgate policy guidance respecting how to clearly and consistently communicate with its partners about what entity the activities are being directed at. As well, I recommended that CSEC ensure that its foreign intelligence analysts are knowledgeable about and follow existing policy guidance, introduced since the period under review, respecting their responsibilities for determining the foreign status of an entity and the justifications for directing activities at that entity. Following the completion of my review, I forwarded to the Chair of SIRC, for information, certain general points relating to CSIS that arose out of the recommendations I made.

At my direction, my office has started a review of other more recent foreign intelligence activities that includes follow-up on matters raised in this review, and will seek to determine whether developments in CSEC policies and procedures since the period under review have led to an improvement in the clarity of language in CSEC information exchanges with CSIS.

Conclusion

As of the end of the 2012–2013 reporting period, March 31, 2013, I am awaiting the Minister's response to the two recommendations. The responses will be noted in next year's annual report.

2. CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the *CSIS Act*

Background

In 2007, CSIS sought from the Federal Court of Canada a warrant to assist in the investigation of threat-related activities that, it was believed, individuals would engage in while travelling outside of Canada. The Honourable Justice Edmond Blanchard held that the Court lacked the jurisdiction to authorize intrusive investigative activities by CSIS employees *outside of Canada* (*Re CSIS Act*, 2008 FC 301).

In 2009, in *X(Re)*, 2009 FC 1058, the Court was asked to revisit the question of jurisdiction and to distinguish Justice Blanchard's reasoning on the basis of a more complete description of the facts relating to the activities necessary to permit the interception and a different legal argument concerning how the method of interception was relevant to the jurisdiction of the Court. The Honourable Justice Richard Mosley was satisfied that there were sufficient factual and legal grounds to distinguish the application from that which was before Justice Blanchard and he issued the first warrant permitting CSIS to intercept the

communications of Canadians located outside Canada using the interception capabilities of CSEC. The application was supported by the affidavit evidence of an employee of CSEC that described the agency's interception capabilities and how communications would be intercepted *from within Canada*.

Paragraph 273.64(1)(*c*) of the *National Defence Act* authorizes CSEC to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. This assistance includes CSEC supporting CSIS with the interception of Canadians' communications if CSIS has a judicially authorized warrant issued under section 21 of the *CSIS Act*. Pursuant to subsection 273.64(3) of the *National Defence Act*, CSEC is subject to any limitations imposed by law on the agency to which it is providing assistance — for example, any conditions imposed by a judge in a warrant. When CSEC provides operational assistance to CSIS, CSEC becomes the agent of CSIS. CSIS is *de jure* the owner of the information and the intercepted communications relating to the subject of the warrant.

In *X(Re)*, Justice Mosley stated:

> Canada has given CSE[C] a mandate to collect foreign intelligence including information from communications and information technology systems and networks abroad. It [CSEC] is restricted as a matter of legislative policy from directing its activities against Canadians or at any person within Canada, but it is not constrained from providing assistance to security and law enforcement agencies acting under lawful authority such as a judicial warrant. CSIS is authorized to collect threat-related information about Canadian persons and others and, as discussed above, is not subject to territorial limitation.
>
> Where the statutory prerequisites of a warrant are met, including prior judicial review, reasonable grounds and particularization of the targets, the collection of the information by CSIS with

> CSE[C] assistance, as proposed, falls within the legislative scheme approved by Parliament and does not offend the *Charter*. (*X(Re)* at paragraphs 75-76)

The objectives of my review were to acquire detailed knowledge of and to document CSEC's assistance to CSIS and to assess whether CSEC activities complied with the law, including with the terms of the warrants issued to CSIS, and any privacy protections found therein. CSEC's assistance to CSIS under the warrants may include use of Canadian identity information and the interception of the communications of Canadians. CSEC's collection, as defined in the warrant, may impact on the privacy of Canadians.

I examined CSEC assistance to CSIS in support of a number of the first warrants of this kind relating to counter-terrorism. Specifically, as part of assessing compliance with the law and privacy protection, for the warrants examined, I verified that:

- CSEC had a copy of the warrant and had clear and sufficient information about the assistance sought by CSIS;
- the communications targeted by CSEC for CSIS were only those communications referred to in the warrants;
- the communications were not targeted before the warrants came into force and were no longer targeted once the warrants expired;
- CSEC targeted the subjects of the warrants only while they were believed to be outside Canada;
- CSEC targeted only the types of communications and information that were authorized in the warrants to be intercepted or obtained; and
- CSEC complied with any other limitations imposed by law on CSIS, for example, any conditions in the warrants.

Findings and recommendations

During the period under review, CSEC responded appropriately to two related privacy incidents it identified involving the unintentional release of Canadian identity information of some of the subjects of the warrants. In fact, CSEC has already clarified appropriate internal processes for the conduct of certain activities and reminded its employees of their information stewardship responsibilities. This should help prevent similar incidents.

I questioned CSEC about another incident involving the interception of communications for CSIS for a small number of days after a particular warrant had expired. I accepted CSEC's explanation for this incident, which was that it resulted from unintentional human error. CSEC also confirmed that these intercepted communications were destroyed and that CSIS did not receive them. I am satisfied that CSEC documented this incident and reminded its employees of proper process to help prevent similar errors.

During the period under review, operational policies and procedures of general application to CSEC's assistance in support of these warrants and related activities were in place and provided direction to CSEC employees respecting compliance with the law and the protection of the privacy of Canadians. Subsequent to the period under review, CSEC issued specific guidance for the conduct of this assistance and activities. Generally, CSEC employees interviewed were well aware of the policies and procedures and demonstrated knowledge of their respective responsibilities. Interviews with CSEC managers, team leaders and other employees showed that managers routinely monitored the assistance and related activities for compliance with governing authorities.

In addition to a detailed examination of CSEC activities under the warrants, I considered and consulted my independent counsel, who is also a privacy law expert, on general questions of law relating to this subject. I made two recommendations to the Minister to help ensure

CSEC assistance to CSIS is consistent with the authorities and limitations of the warrants, and to enhance the measures in place to protect the privacy of Canadians. Specifically, I recommended that:

1. CSEC discuss with CSIS the expansion of an existing practice to protect privacy to other circumstances; and

2. CSEC advise CSIS to provide the Federal Court of Canada with certain additional evidence about the nature and extent of the assistance CSEC may provide to CSIS.

I found that CSEC practices relating to its assistance to CSIS and related activities were consistent with the general requirements in the "Accountability Framework" and "Privacy of Canadians" ministerial directives to CSEC, specifically to comply with the law and to take measures to ensure that information was lawfully obtained and handled in a manner consistent with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*.

Conclusion

While I made two recommendations to the Minister to help ensure CSEC assistance to CSIS is consistent with the law and to enhance privacy protection, I concluded that CSEC conducted its activities in accordance with the law and ministerial direction, and in a manner that included measures to protect the privacy of Canadians. The Minister accepted and CSEC has addressed the recommendations.

Following the completion of my review, I forwarded to the SIRC Chair, for information, certain general points relating to CSIS that arose out of the two recommendations I made and that SIRC may wish to examine as it deems appropriate. Subsequently, CSEC advised me that it raised the recommendations — which relate to matters that are controlled by CSIS, or require agreement from CSIS — with CSIS.

3. Review of CSEC IT security activities not conducted under a ministerial authorization

Background

The *National Defence Act* mandates CSEC to provide advice, guidance and services to Government of Canada departments and agencies as well as to other owners of IT systems to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada (paragraph 273.64(1)(*b*)).

During the period under review, the Government of Canada reorganized its cyber defence efforts. CSEC became the primary point of contact for cyber incidents faced by Government of Canada departments and agencies. Public Safety Canada is the primary point of contact for cyber incidents affecting non-Government of Canada critical infrastructure sectors. A further distinction is that CSEC is responsible for sophisticated cyber threats, such as those stemming from foreign state actors, while Public Safety Canada responds to less sophisticated threats, for example, those relating to known vulnerabilities in commercially available computer software.

I examined certain IT security activities conducted by CSEC to detect, analyse and mitigate cyber threats. CSEC does not undertake these activities under a ministerial authorization as it does not intercept communications. Rather, CSEC uses information acquired by the system owners — under their *Criminal Code* authorities and, for Government of Canada system owners, also under their *Financial Administration Act* authorities — and disclosed to CSEC. These authorities permit the interception of private communications by authorized persons when the interception is reasonably necessary to protect computer systems from mischief and unauthorized use.

The objectives of my review were to assess whether CSEC complied with the law and the extent to which CSEC protected the privacy of Canadians in carrying out the activities. In addition to acquiring detailed knowledge about the activities, I examined:

- the legislative and policy framework for the activities;
- CSEC organizational changes;
- technologies, databases and systems used for the activities;
- the amount and treatment of private communications and Canadian identity information acquired by the activities as well as a sample of those private communications and Canadian identity information used by CSEC; and
- agreements in place with Government of Canada departments and agencies.

Private Communication: "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it" (section 183 of the *Criminal Code*).

I examined activities conducted between April 1, 2009, and March 31, 2011, including a more detailed examination of activities and associated reporting for a number of the departments and agencies assisted by CSEC during that time. Additionally, records were examined to verify that system owner information retained by CSEC was done so under an appropriate legal authority. My review also included an examination of CSEC's responses to areas for follow-up identified in a 2009 study by former Commissioner Gonthier.

Findings

I found that CSEC conducted its activities in accordance with the law and ministerial direction and I had no questions about the reporting and retained information examined.

I suggested that CSEC could enhanse its ability to demonstrate that it has measures to protect the privacy of Canadians by recording the return or deletion of irrelevant information acquired by a system owner and shared with CSEC. Notwithstanding this suggestion, I found that these IT security activities contained satisfactory measures to protect the privacy of Canadians.

During the period under review, operational policies and procedures of general application were in place to provide general direction respecting compliance with the law and the protection of privacy of Canadians. However, there was no specific operational guidance in place for these activities. It is a positive development that, subsequent to the period under review, CSEC issued a specific policy for the conduct of these activities.

Some CSEC employees who were interviewed were unable to cite certain policies, but were aware of the rules governing their activities. In addition, CSEC managers who were interviewed routinely and closely monitored the activities to ensure that their employees complied with governing authorities. Based on the records examined, the answers provided to questions during interviews and CSEC's policy compliance validation activities, the activities reviewed complied with relevant policies and procedures.

Conclusion

My review report contained no recommendations. However, regular in-depth reviews will continue to be conducted of IT security activities not conducted under a ministerial authorization to verify compliance with the law, and the extent to which CSEC protects the privacy of Canadians in carrying out the activities.

4. Review of CSEC's 2010–2011 and 2011–2012 foreign signals intelligence ministerial authorizations

Background

Subsection 273.65(8) of the *National Defence Act* requires the Commissioner to review CSEC activities carried out under ministerial authorizations "to ensure they are authorized and report annually to the Minister [of National Defence] on the review." A regular combined review of the foreign signals intelligence ministerial authorizations is one way that Commissioners fulfill this part of their mandate. This year's review covered two fiscal years: I examined the five foreign signals intelligence ministerial authorizations in effect from December 1, 2010, to November 30, 2011, relating to five activities or classes of activities, as well as the six foreign signals intelligence ministerial authorizations in effect from December 1, 2011, to November 30, 2012, relating to six activities or classes of activities. The purpose of this review was to:

1. ensure that the activities conducted under the ministerial authorizations were authorized and that the Minister was satisfied that the four conditions for authorization required by paragraphs 273.65(2)(*a*) to (*d*) of the *National Defence Act* were met;

2. identify any significant changes to the ministerial authorization documents themselves or to CSEC's activities described in the ministerial authorizations;

3. assess the impact, if any, of these changes on the risk of non-compliance and on the risk to privacy, and, as a result, identify any subjects requiring follow-up review; and

4. examine, for compliance with the law, a sample of my choosing of any resulting private communications unintentionally intercepted by CSEC while conducting foreign signals intelligence collection activities under the ministerial authorizations.

Private communications

The Commissioner monitors the number of private communications unintentionally intercepted and verifies how CSEC treated and used these communications. The Commissioner is able to review all of the private communications that CSEC uses and retains.

Findings

I found that the activities conducted under the 2010–2011 and the 2011–2012 foreign signals intelligence ministerial authorizations were authorized.

For each of the 11 foreign signals intelligence collection activities, I examined certain key information relating to interception and to the privacy of Canadians, to permit comparison of the activities and to identify any significant changes or trends over time. I found no significant changes to the scope or operation of any of the activities to require a follow-up in-depth review of specific activities. The 2010–2011 and 2011–2012 foreign signals intelligence ministerial authorizations did not contain any significant changes from the previous year and CSEC did not make any significant changes to the technologies used for these activities.

Changes made by CSEC in 2010–2011 and in 2011–2012 to its operational policies for foreign signals intelligence collection activities clarified authorities and practices and enhanced the protection of the privacy of Canadians.

I also reviewed a sample of unintentionally intercepted private communications that CSEC recognized and retained, and that CSEC did not use in its reports. I found that in both 2010–2011 and 2011–2012, CSEC retained only those private communications essential to international affairs, defence or security, as required by paragraph 273.65(2)(*d*) of the *National Defence Act*. Again this year, the proportion of these communications remained very small and CSEC destroyed most of them. In addition, a new tool is being developed that will assist CSEC analysts in identifying intercepted communications that might be private communications. The Commissioner's office will examine the impact of this new tool on compliance and privacy protection in a future review.

In last year's report, I indicated that certain information about intercepted communications involving CSEC's international partners was not readily available. It is positive that, while not a requirement in the ministerial authorizations, CSEC has recognized the importance of reporting this information to the Minister. The Commissioner's office will monitor developments.

It is also a positive development that, while not a requirement of a particular ministerial authorization, CSEC has agreed to report to the Minister certain information relating to privacy. This measure to protect the privacy of Canadians will support the Minister in his accountability for CSEC. It also satisfies an outstanding recommendation I made in 2010–2011. The Minister had initially supported CSEC's rejection of this recommendation. However, after further examination, I maintained my recommendation and so informed the Minister. CSEC reconsidered its initial position and advised the Minister that it would undertake to implement the recommendation.

Conclusion

I made no recommendations.

5. Annual review of a sample of disclosures of Canadian identity information to Government of Canada clients

Background

Canadian identity information may be included in CSEC's foreign signals intelligence reports if it is required to understand or use the foreign intelligence. However, any information that identifies a Canadian must be suppressed in the reports — that is, replaced by a generic reference such as "a named Canadian." When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting client has both the authority and operational justification for obtaining the Canadian identity information. Only then may CSEC provide that information.

My officials selected and examined a sample of approximately 20 percent of the total number of disclosures by CSEC to Government of Canada agencies or departments during the period October 2011 to June 2012. The sample included disclosures made to all of the departments that had requested Canadian identity information during the period under review. My officials examined: the requests documenting the clients' authority and justification for obtaining the Canadian identity information; associated CSEC foreign signals intelligence reports; and the actual disclosures of Canadian identity information.

Findings

Based on my assessment of the information reviewed and the interviews conducted, CSEC conducted its disclosure activities in compliance with the law. Operational policies and procedures are in place and provide sufficient direction to CSEC employees respecting the protection of the privacy of Canadians. CSEC employees were knowledgeable about, and acted in accordance with, the policies and procedures.

In addition, in response to a recommendation made by former Commissioner Cory in his 2010 report, in 2012, CSEC started using a new on-line secure system to process requests for and disclosures of Canadian identity information. CSEC provided my employees with a demonstration of the system, which is currently used with CSEC's principal clients. CSEC intends to extend its use to other partners starting in the coming fiscal year. According to CSEC, the system has improved the timeliness of responses and resulted in better service to its clients. It enhances accountability by improving the tracking and retrieval of requests for and disclosures of Canadian identity information and it contains a number of features to help ensure the protection of the privacy of Canadians.

Conclusion

My review did not result in any recommendations. CSEC conducted its disclosure activities in a thorough manner; all of the requests reviewed were authorized, justified and well documented.

Should there be an instance of non-compliance in CSEC disclosure of Canadian identity information, the potential impact on the privacy of Canadians could be significant. For this reason, annual reviews of a sample of disclosures will continue. Next year's sample will include a detailed examination of the use of the new system, as well as a sample of disclosures of Canadian identity information to CSEC's international partners.

6. Annual review of incidents and procedural errors identified by CSEC in 2012 that affected or had the potential to affect the privacy of Canadians and measures taken by CSEC to address them

Background

CSEC maintains a central file describing any operational incidents that did or could have an impact on the privacy of Canadians. CSEC records in this file any incidents it identifies that put at risk the privacy of a Canadian in a manner that runs counter to or is not provided for in its operational policies. CSEC policy requires its foreign signals intelligence and IT security employees to report and document privacy incidents in order to demonstrate compliance with legal requirements and CSEC policies, and to prevent further incidents. Incidents could include, for example, the inadvertent inclusion of Canadian identity information in a report, or mistakenly sharing a report with the wrong recipient.

Horizontal and in-depth reviews of CSEC activities include an examination of any privacy incidents and procedural errors relating to the subject under review and, where appropriate, are reported in the summaries of those reviews. My employees are vigilant during reviews about identifying these types of incidents, so we can confirm whether CSEC also identified and addressed them.

The objectives of this annual review are to: acquire knowledge of the incidents and procedural errors in 2012 and associated actions; and inform development of the Commissioner's work plan, by determining if there are any systemic issues or issues about compliance with the law or the protection of the privacy of Canadians that should be the subject of follow-up review. The review of these privacy incidents and procedural errors also assists in evaluating how CSEC monitors and validates that its activities adhere to its operational policies.

Findings

I examined all foreign signals intelligence and IT security privacy incidents and procedural errors recorded by CSEC in calendar year 2012, and the subsequent actions taken by CSEC to correct them.

There was a very small number of procedural errors and I agreed with CSEC's assessment that these occurrences were minor and did not amount to privacy incidents.

Based my review of CSEC's records as well as independent verification by my office of reports in a CSEC database, I am satisfied that CSEC took appropriate corrective actions in response to the small number of privacy incidents it recorded.

I was particularly pleased with certain remedial actions taken by CSEC to prevent future similar privacy incidents. For example, CSEC is now conducting a monthly review of its central file to ensure that all required remedial activities have been completed or are being pursued. As well, CSEC reminded its employees of the requirement to report an incident immediately. CSEC also established a process to send reminders to its employees to make sure that certain information in its systems is up to date and compliant with existing authorities.

Conclusion

My review of the privacy incidents and procedural errors identified by CSEC in 2012 did not result in any recommendations. My review did not reveal any systemic deficiencies or issues that require follow-up review. Annual reviews will continue to be conducted of the privacy incidents and procedural errors identified by CSEC.

COMPLAINTS ABOUT CSEC ACTIVITIES

In 2012–2013, my office was contacted by a number of individuals who were seeking information or expressing concern about CSEC activities. However, the inquiries were assessed as outside of the Commissioner's mandate or as lacking credibility. No complaints about CSEC activities warranted investigation by the Commissioner. (More information on the complaints process is available on the office's website.)

DUTY UNDER THE *SECURITY OF INFORMATION ACT*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy seeking to defend the release of special operational information — such as certain information relating to CSEC activities — on the grounds that it is in the public interest. No such matters were reported to me in 2012–2013. (More information on the Commissioner's responsibilities under the *Security of Information Act* is available on the office's website.)

ACTIVITIES OF THE COMMISSIONER'S OFFICE

In last year's annual report, in an attempt to clarify misconceptions and to better inform the public about CSEC's and my mandates and activities, I provided more detail than ever before on CSEC's activities, what Commissioners review, how reviews are carried out, and the impact of reviews. Work is ongoing to improve the website, which contains detailed information on the activities of the Commissioner's office. Of course, the Commissioner provides the Minister of National Defence with additional classified information — which cannot be disclosed in this public report or on the website — so that the Minister can be fully aware of the Commissioner's review of CSEC activities. Last year, employees of my office and I also met with a number of academics and other professionals interested in review of security and intelligence agencies to talk about my role and work and their views on effective review. In addition, my office made presentations to five cohorts of new CSEC employees attending

CSEC's foundational learning course, which is a requirement for every new employee. These presentations provide an introduction to what it is I and my office do, how we go about our work, and how it may affect them as CSEC employees.

During the past year, CSEC provided a number of detailed briefings to employees of my office as part of the conduct of reviews. CSEC also provided an overview briefing on recent and important operational, policy and organizational changes and issues. I attended an interactive presentation that demonstrated CSEC's foreign signals intelligence capabilities and response to an incident. The event was very effective in demonstrating how the many different parts of CSEC, many personnel and many different government departments and agencies cooperate, in response to a top Government of Canada priority. I was struck by the knowledge and professionalism of CSEC employees and their evident dedication to their respective responsibilities. In addition, my employees attended CSEC training on foreign signals intelligence activities and on communications security.

Following a conference on security and privacy at the Université de Montréal in October 2011, my office's Executive Director wrote a chapter in a book, *Circulation internationale de l'information et sécurité*, published in late 2012. The chapter was based on his participation in one of the conference panels, describing distinctions between national security and public safety, the role and impact of review, and the integration of technology and privacy protection in national security.

At the beginning of March, the Executive Director delivered a luncheon address at the 15th annual conference organized by the Centre for Military and Strategic Studies at the University of Calgary, with the theme *Global Security: Past, Present and Future*. His address dealt with the role of intelligence review, focussing on four questions: why is review important; how effective can it be and what makes for effective review; what is the view of the intelligence agencies themselves concerning review; and what of the future and some challenges.

WORK PLAN — REVIEWS UNDER WAY AND PLANNED

Commissioners use a risk-based and preventative approach to reviews. A three-year work plan is updated twice a year. Developing the work plan draws on many sources. Two important ones are regular briefings from CSEC on new activities and changes to existing activities, and the Chief of CSEC's classified annual reports to the Minister of National Defence on CSEC's priorities and legal, policy and management issues of significance.

The results of several reviews currently under way are expected to be reported to the Minister of National Defence in the coming year and included in my successor's 2013–2014 annual report. The subjects of these reviews include: CSEC counter-terrorism activities; a follow-up to this year's review of certain foreign signals intelligence activities; CSEC's policy compliance validation framework and activities; and a review of particular signals intelligence collection activities conducted under ministerial authorizations.

In addition, before the end of my term as Commissioner, I will report to the Minister on my ongoing review of CSEC's foreign signals intelligence sharing with its closest international partners — the United States' National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Defence Signals Directorate and the New Zealand Government Communications Security Bureau. CSEC and its international partners respect each other's laws by pledging not to direct collection activities at one another's citizens' communications. CSEC is prohibited from requesting an international partner to undertake activities that CSEC itself is legally prohibited from conducting. However, CSEC sharing information with its international partners could affect a Canadian; it is in the international sharing of personal information where the risks are higher than for sharing involving domestic partners. My 2011–2012 annual report contained an update on

this review. This year, I continued my in-depth review and consulted my independent counsel on general questions of law relating to this subject.

Some of the reviews planned for 2013–2014, which may carry over to the next year, are: a review of CSEC IT security activities conducted under ministerial authorizations in support of Government of Canada efforts to address cyber threats; a follow-up review of CSEC activities carried out under a ministerial directive for the purposes of identifying new foreign entities believed to be of foreign intelligence interest; and a follow-up review of CSEC efforts to address numerous gaps related to CSEC's dealings with the Canadian Armed Forces, as identified by CSEC internal evaluators. In addition, the office plans to continue the annual reviews of: (1) foreign signals intelligence ministerial authorizations; (2) CSEC disclosures of Canadian identity information; and (3) privacy incidents and procedural errors identified by CSEC and the measures subsequently taken by CSEC to address them. The office will work with my successor to put in place a comprehensive work plan soon after his or her appointment.

IN CLOSING

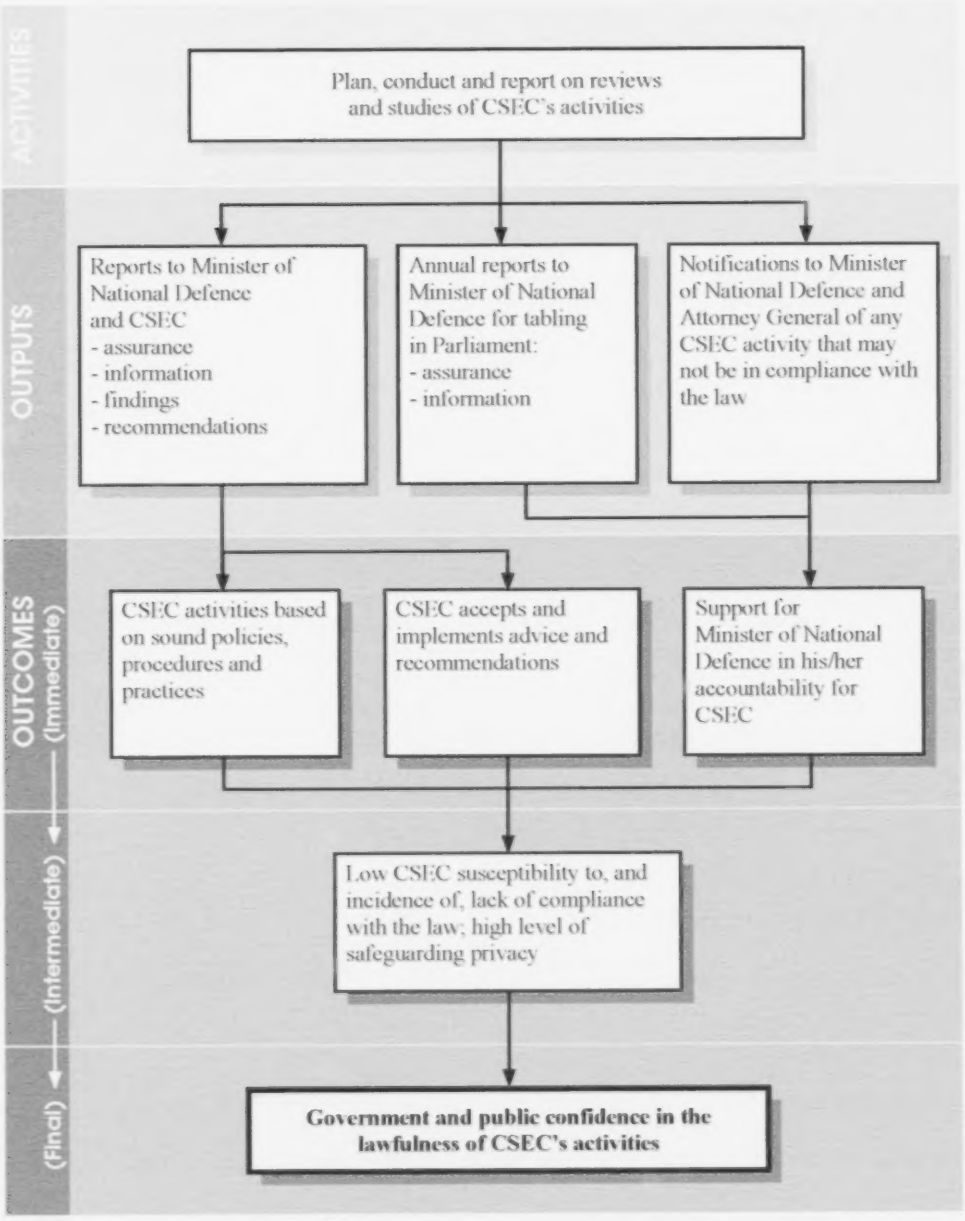
The position of Commissioner is a legislated part of how the government decided, in enacting the *National Defence Act*, to strike a balance between — on the one hand — the Government of Canada's need for foreign signals intelligence and IT security services, and — on the other hand — the need to protect the privacy of Canadians.

The role of the Commissioner and the Commissioner's office is to be sceptical and critical of CSEC activities and it is natural that our respective organizations may sometimes disagree. However, we have a shared objective with CSEC, which is to ensure CSEC complies with the law and protects the privacy of Canadians in the conduct of its activities.

The fulfillment of the Commissioner's mandate rests on the integrity of the office, its ability to effect change at CSEC and inspire confidence in the public that CSEC is under rigorous review.

Finally, I thank the staff of my office, whose dedication, enthusiasm, teamwork, rigour and sense of duty have been nothing short of remarkable these past three years. I can say with pride and confidence that CSEC is truly being watched.

ANNEX A: COMMISSIONER'S OFFICE REVIEW PROGRAM — LOGIC MODEL



ANNEX B: EXCERPTS FROM THE *NATIONAL DEFENCE ACT* AND THE *SECURITY OF INFORMATION ACT* RELATED TO THE COMMISSIONER'S MANDATE

***National Defence Act* — Part V.1**

Appointment of Commissioner

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

Duties

(2) The duties of the Commissioner are

(*a*) to review the activities of the Establishment to ensure that they are in compliance with the law;

(*b*) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(*c*) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

Annual report

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

Powers of investigation

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

Employment of legal counsel, advisors, etc.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

Directions

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

[...]

Review of authorizations

273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

Security of Information Act

Public interest defence

15. (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

Prior disclosure to authorities necessary

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(*b*) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

ANNEX C: 2012–2013 STATEMENT OF EXPENDITURES

Standard Object Summary ($)

Salaries and Benefits	907,567
Transportation and Telecommunications	15,412
Information	59,131
Professional and Special Services	305,572
Rentals	217,803
Repairs and Maintenance	1,515
Material and Supplies	10,383
Machinery and Equipment	16,985
Capital Assets, including Leasehold Improvements	751,350
Total	**2,285,718**